JL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/050,752	01/16/2002	Sean Brennan	16375-00025	7828

21186 7590 04/14/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/050,752	**Applicant(s)** BRENNAN, SEAN	
	Examiner Michael J. Simitoski	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-34* is/are pending in the application.

4a) Of the above claim(s) *1-3,14 and 15* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4,5,7-13 and 16-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 March 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3/3/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. The response of 3/13/2006 was received and considered.

2. The IDS of 3/3/2006 was received and considered.

3. The Drawings of 3/13/2006 are accepted.

4. Claims 4-5, 7-13 & 16-34 are pending.

Response to Arguments

5. Applicant's arguments with respect to claims 4-5, 7-13 & 16-20 have been considered but are moot in view of the new ground(s) of rejection, however, any arguments currently applicable will be addressed.

6. In light of Applicant's amendments to the claims, the rejections under 35 U.S.C. §112, set forth in the previous Office Action, are withdrawn.

7. Applicant's response (p. 10) argues that "there is no teaching or suggestion in either references to apply private/public key encryption to the one-time password generated by the RSA token". However, as stated in the Office Action, RSA discloses that the authentication token is transmitted using SSL (p. 3, §III, ¶2). Further, Stallings teaches that SSL involves a key exchange, for instance RSA key exchange, where a secret key is encrypted with the receivers RSA public key (p. 214). Therefore, as combined, at least one authentication method employs a fixed complex code, which employs a public key infrastructure. If applicant intends a one-time password to be encrypted using a public or private key, this limitation must be recited in the claims.

Election/Restrictions

8. Claims 1-3 7 14-15 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 3/13/2006.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 24-27 & 31-34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

11. Regarding claims 24, 27, 34 & 31, the claims recite the use of both a password and a smart card in the second authentication method, which is not described in the specification.

12. Regarding claims 25-27 & 32-34, the claims recite using a first token to authenticate to a first web site and a second token, one-time password or password/smart card combination to authenticate to a second web site, which is not described in the specification

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 4-5, 7-9, 18, 21 & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,853,980 to Ying et al. (**Ying**) and U.S. Patent Application Publication 2002/0077837 to Krueger et al. (**Krueger**).

Regarding claims 4-5, 7-9 & 18, Ying teaches providing a first user authentication method (col. 23, lines 23-37) and a second authentication method (col. 23, lines 43-46), wherein the first and second user authentication methods are selected to authenticate at least one factor associated with the user/password and credit card information (col. 23, lines 23-37), enabling a user to communicate authentication data to a first web site using the Internet (col. 23, lines 23-50), authenticating the user at the first web site using the first authentication method/user and password (col. 23, lines 23-37), enabling the communication of at least some of the authentication data/credit card information from the first web site to a second web site/credit card processor (col. 23, lines 52-63) using the second authentication method/credit card processing, and wherein both web sites (font web site and credit card processor) are involved in user authentication using the authentication data and wherein access to content/fonts on the first web site is restricted if the user is not authenticated to both web sites (col. 23, line 65 – col. 24, line 5). Ying discloses a second server/credit card processor, but lacks specifically a web site. However, Krueger teaches a first web site/merchant web page (¶40) where authentication information/user and password information and credit card information is entered and transferred from a first web site to an authentication web site/verification system (¶41), wherein the user authenticates a second web site/verification system (¶¶43-44) to gain the benefit of increased security of the user's confidential information (¶9). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to make use of Krueger's system, and as such include credit card information to be sent from Ying's font web site to Krueger's verification system web site, as part of the checkout process, where the user is further authenticated to the verification system web site/verification system web site. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information, as taught by Krueger (¶9).

Regarding claim 21, Ying discloses requiring a user authenticate to a first web site/merchant web site (col. 23, lines 9-37), where the user is granted access to content if authenticated (col. 23, line 65 – col. 24, line 5). Ying's system discloses that once the user is authenticated to the first web site/font web site, the user engages in a credit or debit checkout (col. 23, lines 41-50), but lacks authenticating to a second web site. However, Krueger teaches a first web site/merchant web page (¶40) and authenticating the user to a second web site/verification system (¶¶43-44) to gain the benefit of increased security of the user's confidential information (¶9). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying such that once authenticated to the first web site/merchant web site, authenticate the user to a second web site/verification system site, where the user is granted access to content on the first web site only if authenticated to both the first and second web sites. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information, as taught by Krueger (¶¶9, 43-44 & 61-63).

Regarding claim 28, Ying discloses a first web site/merchant web site (col. 23, lines 9-37), implementing a first authentication method (user/pass), entering authentication information/credit card information and user/password information (col. 23, lines 23-26 & 41-50) via the first web site/merchant web site wherein the user is granted access to content on the first web site/merchant web site only if authenticated to both the first web site and a credit card processor (col. 23, line 41 – col. 24, line 5). Ying lacks an authentication web site implementing a second authentication method, connected to the first web site where authentication information for the second authentication method is transferred from the first web site to the authentication web site and granting access only if the user is authenticated to both the first web site and a second web site. However, Krueger teaches a first web site/merchant web page (¶40) where authentication information/credit card information is entered and transferred from a first web site to an authentication web site/verification system (¶41), wherein the user authenticates a second web site/verification system (¶¶43-44) to gain the benefit of increased security of the user's confidential information (¶9). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to make use of Krueger's system, and as such include credit card information to be sent from Ying's font web site to Krueger's verification system web site, as part of the checkout process, where the user is further authenticated to the verification system web site. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information, as taught by Krueger (¶9).

15. Claims 10-12, 19-20, 22-27 & 29-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ying** and **Krueger**, as applied to claims 21 & 28 above, in further view of "RSA Web Security Portfolio, How RSA SecurID Agents Can Secure Your Website" by **RSA**.

Regarding claims 10-12, Ying lacks one authentication method employing a password. However, RSA teaches that two-factor authentication (p. 2, ¶1), which comprises entering a user ID, PIN and a randomly generated authentication code generated by a token (p. 2, ¶4), ensures greater security than traditional static passwords (p. 2, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying such that the user enters at least a randomly generated authentication code to Ying's font web site, and hence authenticates to the web site using a token. One of ordinary skill in the art would have been motivated to perform such a modification to ensure greater security, as taught by RSA (p. 2, ¶¶1-4).

Regarding claim 19, Ying lacks at least one user authentication method used across multiple web sites. However, RSA teaches using the RSA SecurID system in a mixed Web server environment, where users can traverse between the servers without being re-authenticated by issuing cookies that are valid on multiple servers (p. 3, §Web Single Sign-on). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to utilize RSA SecurID to issue at least one cookie that is valid on multiple servers. One of ordinary skill in the art would have been motivated to perform such a modification to enable users to traverse between the servers without being re-authenticated by issuing cookies that are valid on multiple servers, as taught by RSA (p. 3, §Web Single Sign-on).

Regarding claim 20, Ying lacks explicitly the token being embedded in a cell phone. However, RSA discloses embedding the token in a device such as a cell phone to fit with daily work habits (p. 2, §III, ¶5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying, as modified above, to include the token in a cell phone. One of ordinary skill in the art would have been motivated to perform such a modification because it is known to fit daily work habits, as taught by RSA (p. 2, §III, ¶5).

Regarding claims 22-24 & 29-31, Ying lacks authenticating to the second web site with a token. However, RSA teaches that two-factor authentication (p. 2, ¶1), which comprises entering a user ID, PIN and a randomly generated authentication code generated by a token (p. 2, ¶4), ensures greater security than traditional static passwords (p. 2, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying, as modified above, such that the user enters at least a randomly generated authentication code to Krueger's verification server, and hence authenticates to the second web site using a token. One of ordinary skill in the art would have been motivated to perform such a modification to ensure greater security, as taught by RSA (p. 2, ¶¶1-4).

Regarding claims 25-27 & 32-34, Ying lacks authenticating to the first web site with a first token and authenticating to the second web site with a second token. However, RSA teaches that two-factor authentication (p. 2, ¶1), which comprises entering a user ID, PIN and a randomly generated authentication code generated by a token (p. 2, ¶4), ensures greater security than traditional static passwords (p. 2, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to use RSA two-factor authentication and Krueger to use RSA two-factor authentication. One of ordinary skill in the art would have been motivated to perform such a modification to ensure greater security in both authentication systems, as taught by RSA (p. 2, ¶¶1-4).

16. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Ying**, **Krueger** & **RSA**, as applied to claim 11 above, in further view of U.S. Patent Application Publication 2001/0045451 to Tan et al. (**Tan**) in further view of "eToken: The Key to Security for the Internet Age" by **Aladdin**. RSA lacks explicitly a USB-based token being accessed by a browser. However, Tan teaches that to allow access to a web site using a smart card, the browser can read necessary access information directly from the smart card and pass the information to the server to which the user is authenticating (¶6-11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the RSA security token to communicate electronically with the web browser. One of ordinary skill in the art would have been motivated to perform such a modification to pass the generated code to the server for use in authentication, as taught by Tan (¶6-11). Further, Aladdin teaches that using USB tokens for authentication allows the user to take advantage of the USB ports included in millions of PCs (p. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify RSA to include the SecurID token in a USB-based device. One of ordinary skill in the art would have been motivated to perform such a modification to take advantage of millions of USB-ready PCs for authentication, as taught by Aladdin (p. 1).

17. Claims 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ying, Krueger & RSA**, as applied to claim 4 above, in further view of Network Security Essentials Applications and Standards by **Stallings**. Ying, as modified above by RSA, lacks explicitly that the authentication method employs a fixed complex code which comprises a public key infrastructure. However, RSA discloses that the authentication token is transmitted using SSL (p. 3, §III, ¶2). Further, Stallings teaches that SSL involves a key exchange, for instance RSA key exchange, where a secret key is encrypted with the receivers RSA public key (p. 214). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to explicitly employ a fixed complex code which comprises a public key infrastructure. One of ordinary skill in the art would have been motivated to perform such a modification to utilize an RSA public key to exchange keys, as taught by Stallings (p. 214).

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
April 6, 2006